



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/903,278	07/11/2001	Philip M. Walker	10012790-1	9299

7590 11/27/2007
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P. O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

TRAN, TONGOC

ART UNIT	PAPER NUMBER
----------	--------------

2134

MAIL DATE	DELIVERY MODE
-----------	---------------

11/27/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/903,278
Filing Date: July 11, 2001
Appellant(s): PHILIP M. WALKER

MAILED

NOV 27 2007

Technology Center 2100

James Baudino
Registration No. 43,486
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed August 2, 2007 appealing from the
Office action mailed March 1, 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,978,475	SCHNEIER et al.	11-1999
6,088,804	HILL et al.	7-2000

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-17, 19-24 and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier et al. (U.S. Patent No. 5,978,475).

In respect to claims 1, 10 and 19, Schneier discloses a system and method comprising:

a target; a probe operable to execute in the target and collect a predetermined set of data associated with the target; and a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered (e.g. col. 6, line 41-col. 7, line 19, target, untrusted computer, monitor-trusted computer, a probe-audit log, "transmit it to the trusted computer for verification", "verification-the set of operations done on the logfile to guarantee that it hasn't been altered...", col. 7, lines 14-19).

In respect to claims 2, 11 and 20, Schneier further discloses wherein the probe is resident in the target (e.g. col. 7, lines 5-13).

In respect to claims 3, 12 and 21, Schneier further discloses wherein the monitor is operable to send the probe to the target for execution (e.g. col. 7, lines 5-6).

In respect to claims 4, 13 and 22, Schneier further discloses wherein the probe repeatedly executes and the predetermined set of data varies for each execution of the probe (e.g. col. 7, lines 7-8).

In respect to claim 5, Schneier further discloses wherein the predetermined set of data includes system attributes and system usage data (e.g. col. 1, lines 34-52 and col. 6, lines 51-64).

In respect to claims 6 and 15, Schneier further discloses wherein the probe is operable to calculate a signature value of at least a portion of an execution image of the probe (e.g. col. 8, line 45-col. 9, line 2).

In respect to claims 7 and 16, Schneier further discloses wherein the monitor is operable to compare the calculated signature value to an expected signature value (e.g. col. 8, line 45-col. 9, line 2).

In respect to claims 8, Schneier further discloses wherein the probe is operable to determine a signature value of a random subset of an execution image of the probe (e.g. col. 18, lines 23-28).

In respect to claims 9 and 17, Schneier further discloses wherein the probe is operable to generate an encryption key from the signature value for encrypting the collected predetermined set of data (e.g. col. 8, line 45-col. 9, line 2).

In respect to claims 19 and 26, Schneier further discloses receiving collected data encrypted by the probe using an encryption key derived from a self-hash value, the data including system attribute data and system usage data; from a self-hash value, the data including system attribute data and system usage data; decrypting the encrypted data; and verifying the system attribute

data (e.g. Col. 1, lines 34-52, col. 5, lines 5-20, col. 6, line 51-col. 7, line 19 and col. 8, line 45-col. 9, line 3).

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 10 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Hill et al. (U.S. Patent No. 6,088,804).

In respect to claims 1, 10 and 19, Hill discloses a system and method comprising:

a target; a probe operable to execute in the target and collect a predetermined set of data associated with the target; and a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered (e.g. col. 3, lines 1-16, col. 4, lines 30-41, security agent-probe, security event-set of data items associated with the target, col. 5, lines 46-52, col. 4-22, node-target, agents send info. for collection and comparison).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 18 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (U.S. Patent No. 5,978,475).

In respect to claims 18 and 25, Schneier further discloses sending the encrypted data to a monitor, the data including system attribute data and system usage data; Decrypting the encrypted data using a decryption key; Verifying the system attribute data; and (e.g. Col. 1, lines 34-52 and col. 6, line 51-col. 7, line 19, col. 8, line 45-col. 9, line 3). Schneier does not disclose generating billing data based on the system usage data in response to the system attribute data being verified. However, Office Notice is taken that generating billing according to system usage is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement security audit logging and verifying operation taught by Schneier to generate billing according to the information for billing purposes.

(10) Response to Argument

Response to remarks on Rejection under 35 U.S.C. 102(b) over Schneier:

Claim 1:

Claim 1 recites: *"[a] system comprising: a target; a probe operable to execute in the target and collect a predetermined set of data associated with the target; and a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered."*

Response to Appellants' remarks on pages 5 and 6 of the Brief:

Appellants contends that the cited prior art, Schneier, *"appears to be directed toward determining whether the audit log 300 has been tampered with or altered, and not whether the "target" or, in Schneier, the untrusted computer, has been altered. Thus based on the foregoing, the Schneier reference appears to be directed toward determining whether the "predetermined set of data" (the audit log 300) is altered, instead of whether the untrusted computer 102 of Schneier (the "target") has been altered. Accordingly, for at least this reason, Appellants respectfully submit that Schneier does not anticipate Claim 1"*.

In the Specification, Appellants discloses "[i]t is desirable to provide a way to verify the computer system attributes to ensure that the usage accounting and reporting of the system have not been altered in an unauthorized manner. The present invention either sends a probe program to the target computer system or remotely invokes a probe program resident at the target computer to check on a

number of system attributes and generate status data (*Specification, page 3, lines 5-9*); "...probe 20 gets attribute data associated with the client systems such as verification data and billing data. Verification data comprises any information acquired or inferred by the process of sampling and/or modifying various aspects of the target system, involving physical hardware state and/or system files...system attributes and parameters may include a serial number of the CPU (central processing unit) or another program component, the current disk type, the date, size, or other parameters of a specific set of system files, the physical position on a disk drive of certain system files, the network MAC (media access control) address, etc." (*Specification, page 4, lines 1-13*).

Based on this embodiment of the disclosure, the verification is to determine whether information associated with the target (or the client system) has been altered. The verification of the claimed invention involved the monitor receiving a set of data (predetermined data) and it is compared with a second set of data (expected data), the result will determine whether the information associated with the target system has been altered in an unauthorized manner. Therefore, it is the attributes or data obtained by the probe that is being compared and not hardware per se.

Furthermore, Appellants contend that "[c]laim 1 recites "a monitor operable to receive the collected predetermined set of data to compare with expected data values to determine whether the target has been altered".

Appellants state that "Schneier appears to disclose that the audit log 300 of Schneier is a collection of entries indicating, for example, a type of action that is

being logged, the person or computer that initiated the action, the results or effects of the action, successful log-ins, log-offs, remote log-ins, etc. (Schneier, column 6, lines 42-64). Thus, the audit log 300 of Schneier appears to be data representative of entirely unexpected or random occurrences associated with a computer in Schneier. Thus Appellants respectfully submit that the audit log 300 of Schneier is not "compare[d] with expected values" as recited by Claim 1 (emphasis added) to determine "whether the target computer in Schneier has been altered at least because the information of the audit log 300 of Schneier appears to be completely unexpected and/or random based on what acts or events happen to take place or occur with the computer of Schneier. Therefore, for at least this reason also, Appellants respectfully submit that Claim 1 is not anticipated by Schneier.

The phrase "predetermined set of data" and "expected data values" represent a relative data set as referencing in the embodiment mentioned before. For example, the attributes associated with the target system may represent verification data or billing data (e.g. col. 1, lines 15-19). Similarly, Schneier discloses using different authentication and verification techniques to determine whether the log files has been altered (e.g. col. 7, lines 15-19 and col. 8, line 44-col. 9, line 30). Schneier discloses "[m]any modern audit logs are often kept in digital files on computer. Examples of such computer audit logs include but are not limited to:" (Schneier, col. 1, lines 34-51); "In general, the logged event information 201, may be any information that can be presented in digital form.

For any particular event, this will depend heavily on the application (Schneier, col. 6, lines 51-53).

Claim 10:

Claim 10 recites: "[a] method comprising: executing a probe in a target; collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered."

The argument presented in the Brief is similar to the argument presented in Claim 1. Therefore, the response to Claim 1 above also applies to Claim 10.

Response to Appellants' remarks on pages 7 and 8 of the Brief:

Claim 6:

Claim 6 recites "the system, as set forth in claim 1, wherein the probe is operable to calculate a signature value of at least portion of an execution image of the probe".

Appellants contend that Schneier does not disclose the cited limitation. Schneier discloses tools for implementing various cryptographic techniques (i.e. col. 5, lines 6-21, col. 8, line 44-col. 9, line 30 and col. 15, lines 25-34); "Cryptographic module 165 has the ability to perform a variety of functions required by the auditing program 200. Such functions include, but are not limited to: 1) a one-way hash function, such as SHA-1, MD5, or RIPE-MD 160..." (i.e. col. 5, lines 6-9); "an auditing program 200, including a user module 210, a cryptographic module 220, and a file storage module 240 (i.e. col. 6, lines 12-14);

"File storage module 230 obtains (inputs) the selected information to be logged and data to be hashed from file storage device 160 or remotely via external interface 180, as appropriate (i.e. Fig. 1B, col. 6, lines 28-31); "Another disadvantage of conventional techniques is that they do not work when the software creating the audit log does not trust the machine or network it is running on. This situation might occur when a Java-like Internet application is running on an unsecured remote machine or over an insecure network, when a software "agent" is running on a hardware device whose tamper-resistance features are not reliable (i.e. col. 2, lines 7-15).

The claimed limitation referring the "target" as "client" system or "untrusted" system as Appellants explained in Brief, if this is the case, the auditing program residing in the untrusted system would have been suggested by Schneier as having necessary cryptographic protection or tamper-resistant in order to ensure when sensitive information must be kept on an untrusted machine ("U") that is not physically secure or sufficiently tamper-resistant to guarantee that it can not be taken over by some attacker. Because Schneier does teach that the cryptographic module can be implemented as a local software or as remote software, it suggests that the protective measure such as the well known techniques described by the various cryptographic tools used to implement this protective measure to ensure the sensitive information resided in the untrusted machine can be protected. Furthermore, Schneier discloses that "the untrusted computer might be a consumer's electronic wallet" (col. 5, lines 60-61). As is well known for limited memory in smaller device such as

consumer's electronic wallet, it would be impractical to perform cryptographic operation without consideration of the selected information to be implemented on or what cryptographic options are to be used to protect the information (i.e. col. 6, lines 12-20).

Claim 8:

The claim limitation and arguments presented in the Brief is similar to the arguments presented in Claim 6. Therefore, the response to Claim 6 above also applies to Claim 8.

Claim 15:

The claim limitation and arguments presented in the Brief is similar to the arguments presented in Claim 6. Therefore, the response to Claim 6 above also applies to Claim 15.

Claim 16:

The claim limitation and arguments presented in the Brief is similar to the arguments presented in Claim 6. Therefore, the response to Claim 6 above also applies to Claim 16.

Response to remarks on Rejection under 35 U.S.C. 102(b) over Hill:

Claim 1:

Response to Appellants remarks on page 9 in the Brief:

Appellants contend that the cited prior art, Hill, does not disclose the monitor "receive[s] the collected predetermined set of data to compare with expected data values to determine whether the target has been altered".

Appellants further contend that "the SOM processor 40 of Hill appears to compare a signature received from the security agent 36 of Hill to determine a recommended action or response to the attack (Hill, Abstract, column 8, lines 35-53, column 10, lines 24-36). Hill appears to disclose that the security events may include port scans, malicious software, penetration attempts, etc. (Hill, column 4, lines 31-41). Thus the SOM processor 40 of Hill does not make any comparison "to determine" whether the target has been altered as recited by Claim 1. To the contrary, the SOM processor 40 is merely determining what action or response to take to an identified attack. Thus, Appellants submit that the SOM processor 40 of Hill is not making any comparison "to determine whether the target has been altered" as recited by Claim 1. Thus, for at least this reason, Appellants submit that Hill does not anticipated Claim 1."

Hill discloses the SOM processor (correspondence to the monitor of claimed invention) maps a vector representative of first training signature 54 into display cell 68' which is located in middle region 72. Thus the division of display map 66 into regions 70, 72, and 74 and subregions 76 indicates attack type and attack severity. When actual attack information from network 22 is then compared to display map 66, a network manager is provided with attack type and severity in a quickly interpretable form (i.e. col. 7, lines 1-8). The indications of attack type and attack severity encompass determining whether the target computer has been altered.

Claim 10:

Response to Appellants remarks on page 10 in the Brief:

Claim 10 recites: "[a] method comprising: executing a probe in a target; collecting a predetermined set of data associated with the target for comparison with expected data values for the predetermined set of data to determine whether the target has been altered."

The argument presented in the Brief with respect to rejection under Hill to claim 10 is similar to the argument presented in Claim 1. Therefore, the response to Claim 1 above also applies to Claim 10.

Claim 19:

Response to Appellants remarks on pages 10 and 11 in the Brief:

Claim 19 recites "[a] method comprising:

Initiating the execution of a probe in a target;

Receiving from the probe a predetermined set of data associated with the target; and

Comparing the received predetermined set of data associated with expected data values thereof to determine whether the target has been altered.

The argument presented in the Brief with respect to rejection under Hill to claim 19 is similar to the argument presented in Claim 1. Therefore, the response to Claim 1 above also applies to Claim 19.

Response to remarks on Rejection under 35 U.S.C. 103:

Claims 18 and 25:

Response to Appellants remarks on pages 11 and 12 in the Brief:

Appellants state that "[c]laims 18 and 25 depend respectively from independent Claims 10 and 19. As indicated above, Claims 10 and 19 are patentable over Schneier. Therefore, for at least this reason, Claims 18 and 19 are also patentable over Schneier". Since Appellants' remarks in the Brief with respect to claims 10 and 19 are similar to arguments presented in claim 1, the same response to claim 1 also applied to dependent claims 10 and 19 and dependent claims 18 and 25 since the claimed language of the dependent claims contain language of the independent claims 10 and 19.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Respectfully submitted,

/Tongoc Tran/
Tongoc Tran
Patent Examiner
AU: 2134

Application/Control Number:
09/903,278
Art Unit: 2134


Page 17

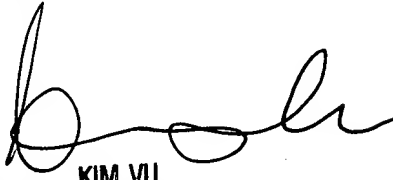
Conferees:

Kambiz Zand
SPE
AU: 2134



KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Kim Vu 
SPE
AU: 2135



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100